UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JASON DOZAL, individually and on behalf of all others similarly situated, Plaintiff, v. FINANCIAL BUSINESS AND CONSUMER SOLUTIONS, INC., Defendant.	**Case No. 2:24-cv-2775** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jason Dozal, individually and on behalf of all others similarly situated, brings this Class Action Complaint and allege the following against defendant Financial Business and Consumer Solutions, Inc. ("FBCS" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this class action against FBCS for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI"). The PII and PHI may have included victims' names, addresses, Social Security numbers, driver's license numbers, financial information (*e.g.*, account numbers, credit or debit card numbers), medical information, health insurance information, dates of birth, and more.

2. FBCS failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiff seeks, among other things, orders requiring FBCS to fully and accurately disclose the nature of the information that has been compromised and to adopt

sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. On February 26, 2024, FBCS "discovered unauthorized access to certain systems in its network." Its subsequent investigation determined that the access persisted from February 14 and February 26, 2024. But FBCS did not disclose the incident until April 26, 2024, when it reported having sent notification letters to people whose PII was exposed by the Data Breach. That disclosure also reflected that 1,955,385 persons were affected by the breach.

4. On June 20, 2024, FBCS disclosed that 3,435,640 persons were in fact affected by the Data Breach.

5. FBCS knowingly obtained sensitive PII and PHI and had a resulting duty to securely maintain that information in confidence. Plaintiff and Class Members would not have provided their PII and PHI to FBCS if they had known that FBCS would not ensure that it used adequate security measures.

6. Plaintiff seeks to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and PHI were exposed in the Data Breach. Plaintiff seeks remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to FBCS's data security policies and practices.

PARTIES

7. Plaintiff Jason Dozal is a resident of Nampa, Idaho. Mr. Dozal received a letter from FBCS dated May 10, 2024, which reported that the Data Breach resulted in the disclosure of information that affected his "Name, Address, Social Security Number/Tax Identification Number, and Date of Birth."

8. Defendant Financial Business and Consumer Solutions, Inc. is a Pennsylvania corporation, with its principal place of business in Hatboro, Pennsylvania.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a state other than Pennsylvania, there are more than 100 class members, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

10. This Court has personal jurisdiction over FBCS because FBCS maintains its principal place of business in Pennsylvania and conducts substantial business in this District; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and because FBCS resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

The Data Breach

12. FBCS describes itself as "nationally licensed and bonded collection agency offering pre-charge off, early out, and third party collection services for clients across a variety of industry verticals," and claims that its "diverse experience enables us to provide our clients

with the financial performance they need, while minimizing risk..”[1] FBCS maintains satellite offices in Cape May, New Jersey and Tampa, Florida.[2]

13. Due to the nature of the services it provides, FBCS acquires and electronically stores PII and PHI. FBCS was therefore required to ensure that PII and PHI were not disclosed or disseminated to unauthorized third parties without Plaintiff’s and Class Members’ express written consent.

14. On April 26, 2024, FBCS notified the Maine Attorney General that “unauthorized actor had the ability to view or acquire certain information on the FBCS network” between February 14 and February 26, 2024.[3] FBCS further reported that “[t]he information that could have been subject to unauthorized access includes name, Social Security number, date of birth, and account information.”

15. On or around April 29, 2024, FBCS notified the Texas Attorney General of the Data Breach. That notification reflected the exposure of far more information than what was reflected in FBCS’s previous notification, i.e., names, addresses, Social Security numbers, driver’s license numbers, financial information (*e.g.*, account numbers, credit or debit card numbers), medical information, health insurance information, dates of birth, and more.[4] That notification also reflected that 230,242 Texans were affected by the Data Breach.[5]

---

[1] About Us, available at https://www.fbcs-inc.com/about-fbcs-collection-agency/ (last visited Apr. 29, 2024).

[2] *Id.*

[3] Notice, available at https://apps.web.maine.gov/online/aeviewer/ME/40/5fe1ede5-aafd-4da2-b1a4-0057a6cdadc6/8e30c591-6126-4644-a9eb-5a9f1f9ee2f7/document.html (last visited May 10, 2024).

[4] Data Security Breach Reports, available at https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited May 10, 2024).

[5] *Id.*

16. On May 10, 2024, FBCS disclosed to the Maine Attorney General that 2,679,555 persons were affected by the Data Breach.[6]

17. FBCS's disclosures are deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what FBCS knows about the degree to which the data has been disseminated.

18. FBCS has not disclosed nearly all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, FBCS has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff's and Class Members' interests, and ensure that FBCS has proper measures in place to prevent similar incidents from occurring in the future.

FBCS's Security Representations

19. FBCS's website includes a short "Privacy Policy," which claims that "FBCS, Inc. takes your privacy and security very seriously and has put significant privacy and security protections in place for our consumers, clients, and employees. These protections are designed utilizing industry privacy and security best practices to ensure your personal information is protected."[7]

---

[6] *See* Data Breach Notifications, available at https://apps.web.maine.gov/online/aeviewer/ME/40/47ea0bb7-cdf0-4fd4-b2b5-06d285ddf9a0.shtml (last visited May 13, 2024).

[7] Privacy Policy, available at https://www.fbcs-inc.com/privacy-policy/ (last visited May 10, 2024).

20. Despite its responsibility for protecting the PII and PHI of millions of consumers, FBCS has evidently disclosed nothing further about its purported policies for doing so.

FBCS Stores Plaintiff's and Class Members' PII and PHI

21. FBCS obtained and stored a massive amount of PII and PHI. As a condition of using their services, FBCS's clients required that consumers entrust them with highly confidential PII and PHI.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, FBCS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI, and relied on FBCS to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

24. FBCS was aware that the PII and PHI it collected are highly sensitive and of significant value to those who would use it for wrongful purposes.

25. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[8] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web."

[8] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed May 10, 2024).

26. The ramifications of FBCS's failure to keep Plaintiff's and Class Members' PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

27. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

28. FBCS knew, or should have known, the importance of safeguarding PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members because of a breach. FBCS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

29. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

30. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, FBCS's policies and practices with respect to maintaining the security of Plaintiff's and Class Members' PII and PHI were reckless, or at the very least, negligent.

31. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff

and Class Members should be compensated for the time they have expended because of FBCS's misfeasance.

32. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[9]

33. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

FBCS's Lax Security Violates HIPAA

---

[9] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Jan. 18, 2024).

34. FBCS had a non-delegable duty to ensure that all PHI it collected and stored was secure.

35. FBCS is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

36. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

37. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

38. HIPAA requires that FBCS implement appropriate safeguards for this information.

39. Despite these requirements, FBCS failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, FBCS failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff's and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

40. FBCS failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff's and Class Members' PHI.

FBCS Violated FTC Guidelines

41. The Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibited FBCS from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain

reasonable and appropriate data security for consumers' PII and PHI is an "unfair practice" in violation of the FTC Act. *See, e.g., Fed. Trade Comm'n v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

42. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[10]

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[11] The guidelines reflect that businesses should protect the PII and PHI that they keep; properly dispose of PII and PHI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

44. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[12]

45. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and

---

[10] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed May 10, 2024).

[11] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed May 10, 2024).

[12] FTC, *Start With Security*, *supra*.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. FBCS failed to properly implement basic data security practices. FBCS's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. FBCS was at all times fully aware of its obligation to protect Plaintiff's and Class Members' PII and PHI because of its position as a healthcare services provider. FBCS was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

48. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All persons in the United States and its territories whose PII and/or PHI was compromised in the Data Breach.

49. Excluded from the Class are FBCS, any entity in which FBCS has a controlling interest, and FBCS's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

50. Plaintiff reserves the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiff.

51. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. FBCS disclosed that the Data Breach affected at least 1,955,385

individuals. All Class Members' names and addresses are available from FBCS's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

52. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent FBCS had a duty to protect the PII and PHI of Class Members;

b. Whether FBCS was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI;

c. Whether FBCS had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether FBCS took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether FBCS failed to adequately safeguard the PII and PHI of Class Members;

f. Whether FBCS failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether FBCS adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of FBCS's wrongful conduct;

i. Whether Plaintiff and Class Members are entitled to restitution because of FBCS's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

53. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was disclosed by FBCS.

Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through FBCS's common misconduct. Plaintiff is advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

54. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against FBCS to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

55. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because FBCS has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. FBCS's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on FBCS's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

56. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like FBCS. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

57. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because FBCS would necessarily gain an unconscionable advantage in non-class litigation, since FBCS would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

58. The litigation of Plaintiff's claims is manageable. FBCS's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

59. Adequate notice can be given to Class Members directly using information maintained in FBCS's records.

60. Unless a class-wide injunction is issued, FBCS may continue to maintain inadequate security with respect to the PII and PHI of Class Members, FBCS may continue to

refuse to provide proper notification to Class Members regarding the Data Breach, and FBCS may continue to act unlawfully as set forth in this Complaint.

61. FBCS has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
NEGLIGENCE
(on behalf of Plaintiff and the Class)

62. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

63. FBCS knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing FBCS's security protocols to ensure that Plaintiff's and Class Members' PII and PHI in FBCS's possession was adequately secured and protected, that Plaintiff's and Class Members' PII and PHI on FBCS's networks was not accessible to criminals without authorization, and that FBCS's employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiff's and Class Members' PII and PHI.

64. Plaintiff and Class Members entrusted their PII and PHI to FBCS with the understanding that FBCS would safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

65. FBCS knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiff's and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

66. FBCS also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII and PHI.

67. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape.

68. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. FBCS knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class Members' PII and PHI, the critical importance of providing adequate security of that information, the necessity for encrypting PII and PHI stored on FBCS's systems, and that it had inadequate IT security protocols in place to secure Plaintiff's and Class Members' PII and PHI.

69. FBCS's misconduct created a foreseeable risk of harm to Plaintiff and Class Members. FBCS's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

70. Plaintiff and Class Members had no ability to protect their PII and PHI that was in FBCS's possession.

71. FBCS was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

72. FBCS had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

73. FBCS had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

74. FBCS systematically failed to provide adequate security for data in its possession.

75. FBCS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII and PHI within its possession.

76. FBCS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII and PHI.

77. FBCS, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII and PHI within its possession might have been compromised and precisely the type of information compromised.

78. FBCS's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII and PHI to be compromised.

79. But for all of FBCS's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiff's and Class Members' PII and PHI would not have been compromised.

80. Plaintiff never transmitted his own unencrypted PII and PHI over the Internet or any other unsecured source.

81. Following the Data Breach, Plaintiff's PII and PHI has been seized by unauthorized third parties who are now free to exploit and misuse that PII and PHI, and Plaintiff is unable to prevent its further dissemination. Plaintiff's PII and PHI are forever compromised.

82. But for the Data Breach, Plaintiff would not have incurred the loss and publication of his PII and PHI and other injuries.

83. There is a close causal connection between FBCS's failure to implement security measures to protect Plaintiff's and Class Members' PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members. Plaintiff's and Class Members' PII and PHI were accessed and compromised as the proximate result of FBCS's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures and encryption.

84. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

85. As a result of FBCS's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which are still in the possession of third parties, will be used for fraudulent purposes.

86. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

87. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling FBCS to institute appropriate data collection and safeguarding methods and policies with regard to PII and PHI; and (2) compelling FBCS to provide detailed and specific disclosure of what types of PII and PHI have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE *PER SE*
(on behalf of Plaintiff and the Class)

88. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

89. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as FBCS for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of FBCS's duty.

90. FBCS violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. FBCS's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving that PII and PHI.

91. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

92. FBCS's violation of Section 5 of the FTC Act constitutes negligence *per se*.

93. FBCS is an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

94. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, FBCS had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class Members' electronic PHI.

95. Specifically, HIPAA required FBCS to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d)

ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq.*

96. FBCS violated HIPAA by actively disclosing Plaintiff's and Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

97. Plaintiff and Class Members are patients within the class of persons HIPAA was intended to protect.

98. FBCS's violation of HIPAA constitutes negligence *per se*.

99. The harm that has occurred as a result of FBCS's conduct is the type of harm that the HIPAA was intended to guard against.

100. As a direct and proximate result of FBCS's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
BREACH OF EXPRESS CONTRACT
(on behalf of Plaintiff and the Class)

101. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

102. Plaintiff and Class Members entered into valid and enforceable contracts through which they paid money to FBCS in exchange for services. Those contracts included promises by FBCS to secure, safeguard, and not disclose Plaintiff's and Class Members' PII and PHI.

103. FBCS's Notice of Privacy Practices memorialized the rights and obligations of FBCS and its affiliates' patients. This document was, upon information and belief, provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services..

104. In the Notice of Privacy Practices, FBCS commits to protecting the privacy and security of PII and PHI and promises to never share Plaintiff's and Class Members' PII and PHI except under certain limited circumstances.

105. Plaintiff and Class Members fully performed their obligations under their contracts with FBCS.

106. However, FBCS did not secure, safeguard, and/or keep private Plaintiff's and Class Members' PII and PHI. FBCS therefore breached its contracts with Plaintiff and Class Members.

107. FBCS allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' PII and PHI without permission. FBCS therefore breached its Privacy Policy as it pertained to Plaintiff and Class Members.

108. FBCS's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, diminished the value of the services FBCS provided to Plaintiff and Class Members.

109. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including by FBCS's failure to fully perform its part of its bargain with Plaintiff and Class Members.

110. As a direct and proximate result of FBCS's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(on behalf of Plaintiff and the Class)

111. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

112. FBCS had valid contracts with each of its clients. A principal purpose of those contracts was to securely store, transmit and safeguard the Plaintiff's and Class Members' PII and PHI.

113. Upon information and belief, FBCS and each of its contracting clients expressed an intention that Plaintiff and Class Members were intended third-party beneficiaries of these agreements.

114. Plaintiff and Class Members are also intended third-party beneficiaries of these agreements because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances are such that FBCS presumably intended to give the beneficiaries the benefit of the promised performance.

115. FBCS breached its agreements with its clients by allowing the Data Breach to occur, and as otherwise set forth herein.

116. FBCS's breach caused foreseeable and material damages to Plaintiff and Class Members.

COUNT V
UNJUST ENRICHMENT
(on behalf of Plaintiff and the Class)

117. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

118. Plaintiff and Class Members have an interest, both equitable and legal, in their PII and PHI that was conferred upon, collected by, and maintained by FBCS and that was stolen in the Data Breach.

119. FBCS benefitted from the conferral upon it of Plaintiff's and Class Members' PII and PHI, and by its ability to retain and use that information. FBCS understood that it so benefitted.

120. FBCS also understood and appreciated that Plaintiff's and Class Members' PII and PHI was private and confidential and that its value depended upon FBCS maintaining its privacy and confidentiality.

121. But for FBCS's willingness and commitment to maintain its privacy and confidentiality, that PII and PHI would not have been transferred to and entrusted with FBCS. Further, if FBCS had disclosed that its data security measures were inadequate, FBCS would not have been permitted to continue in operation by regulators and the financial marketplace.

122. As a result of FBCS's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff's and Class Members' PII and PHI without having adequate data security measures, and its other conduct facilitating the theft of that PII and PHI), FBCS has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

123. FBCS's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff's and Class Members' sensitive PII and PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

124. Under the common law doctrine of unjust enrichment, it is inequitable for FBCS to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff's and Class Members' PII and PHI in an unfair and unconscionable manner. FBCS's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

125. The benefit conferred upon, received, and enjoyed by FBCS was not conferred officiously or gratuitously, and it would be inequitable and unjust for FBCS to retain the benefit.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(on behalf of Plaintiff and the Class)

126. Plaintiff re-alleges and incorporates by reference herein all the allegations contained in the preceding paragraphs.

127. FBCS owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

128. FBCS still stores Plaintiff's and Class Members' PII and PHI.

129. Since the Data Breach, FBCS has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

130. FBCS has not satisfied its legal duties to Plaintiff and Class Members.

131. Actual harm has arisen in the wake of the Data Breach regarding FBCS's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and FBCS's failure to address the security failings that led to that exposure.

132. Plaintiff, therefore, seeks a declaration: (a) that FBCS's existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, FBCS must implement and maintain reasonable security measures, including, but not limited to, the following:

a. ordering that FBCS engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on FBCS's systems on a periodic basis, and ordering FBCS to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that FBCS engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that FBCS audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that FBCS segment PII and PHI by, among other things, creating firewalls and access controls so that if one area of FBCS's system is compromised, hackers cannot gain access to other portions of FBCS's system;

e. ordering that FBCS purge, delete, and destroy in a reasonably secure manner PII and PHI not necessary for its provision of services;

f. ordering that FBCS conduct regular computer system scanning and security checks; and

g. ordering that FBCS routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiff and his counsel to represent the Class;

b. for equitable relief enjoining FBCS from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling FBCS to use appropriate cybersecurity methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

e. for an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 25, 2024

Respectfully submitted,

/s/ Bart D. Cohen

Bart D. Cohen (PA Bar No. 57606)
BAILEY GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
Phone: (215) 274-9420
bcohen@baileyglasser.com

Attorneys for Plaintiff and the Proposed Class